#5

5

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application of:	)	For: METHOD OF SECURIZATION UTILIZING
MAURICE MILGRAM	)	OPTICAL TRANSMISSION OF INFORMATION
Serial No: 09/900,716	)	
Filed: July 6, 2001	)	Group Art Unit unknown
	)	Examiner: unknown

TRANSMITTAL OF PRIORITY DOCUMENT

Commissioner for Patents
Washington, D.C. 20231

Sir:

Enclosed are certified copies of French Patent Application Nos. 0106177 and 0008898, filed May 10, 2001 and July 7, 2000, upon which priority of the instant application is claimed under 35 U.S.C. §119.

Respectfully submitted,

MARSHALL, GERSTEIN & BORUN
6300 Sears Tower
233 South Wacker Drive
Chicago, Illinois 60606-6357
(312) 474-6300

By: _____
Thomas A. Miller
Reg. No: 40,091

October 15, 2001

5

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 11 JUIL. 2001

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS cedex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30
http://www.inpi.fr

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*01

REQUÊTE EN DÉLIVRANCE 1/2

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 W /260899

Réservé à l'INPI

REMISE DES PIÈCES
DATE 7 JUIL 2000
LIEU 75 INPI PARIS
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0008898
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 07 JUIL. 2000

Vos références pour ce dossier *(facultatif)* BFF000229

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET PLASSERAUD

84, rue d'Amsterdam
75440 PARIS CEDEX 09

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date / /
ou demande de certificat d'utilité initiale	N° Date / /
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date / /

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE SECURISATION UTILISANT UN SUPPORT PORTATIF DE DONNEES NUMERIQUES ET DISQUE OPTIQUE POUR LA MISE EN OEUVRE DE CE PROCEDE.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	Pays ou organisation Date / / N°
	☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR		☐ **S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»**
Nom ou dénomination sociale		DIXET
Prénoms		
Forme juridique		Société à Responsabilité Limitée
N° SIREN		424276459
Code APE-NAF		
Adresse	Rue	2, avenue Michel de Cimiez Villa d'Auvare 06000 NICE
	Code postal et ville	
Pays		FRANCE
Nationalité		Française
N° de téléphone *(facultatif)*		
N° de télécopie *(facultatif)*		
Adresse électronique *(facultatif)*		

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE 2/2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 7 JUIL 2000
LIEU 75 INPI PARIS

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0008898

DB 540 W /260899

Vos références pour ce dossier : *(facultatif)*	BFF000229
6 **MANDATAIRE**	
Nom	
Prénom	
Cabinet ou Société	Cabinet PLASSERAUD
N °de pouvoir permanent et/ou de lien contractuel	
Adresse — Rue	84, rue d'Amsterdam
Adresse — Code postal et ville	75009 PARIS
N° de téléphone *(facultatif)*	
N° de télécopie *(facultatif)*	
Adresse électronique *(facultatif)*	
7 **INVENTEUR (S)**	
Les inventeurs sont les demandeurs	☐ Oui ☒ Non **Dans ce cas fournir une désignation d'inventeur(s) séparée**
8 **RAPPORT DE RECHERCHE**	**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé	☒ ☐
Paiement échelonné de la redevance	**Paiement en deux versements, uniquement pour les personnes physiques** ☐ Oui ☐ Non
9 **RÉDUCTION DU TAUX DES REDEVANCES**	**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Requise antérieurement à ce dépôt *(joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :*
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes	

10 **SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)** Eric BURBAUD 94-0304	**VISA DE LA PRÉFECTURE OU DE L'INPI** M. ROCHET

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11235*02

DÉSIGNATION D'INVENTEUR(S) Page N° 1 / 1

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W /260899

Vos références pour ce dossier *(facultatif)*	BFF000229
N° D'ENREGISTREMENT NATIONAL	0008898

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

PROCEDE DE SECURISATION UTILISANT UN SUPPORT PORTATIF DE DONNEES NUMERIQUES ET DISQUE OPTIQUE POUR LA MISE EN OEUVRE DE CE PROCEDE.

LE(S) DEMANDEUR(S) :

DIXET

DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).

Nom		MILGRAM Maurice
Prénoms		
Adresse	Rue	7 place Pinel 75013 PARIS FRANCE
	Code postal et ville	
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)

Le 7 juillet 2000

CABINET PLASSERAUD

Eric BURBAUD

94-0304

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Procédé de sécurisation utilisant un support portatif de données numériques et disque optique pour la mise en œuvre de ce procédé.

La présente invention est relative aux procédés de sécurisation utilisant des supports portatifs de données numériques et aux disques optiques pour la mise en œuvre de ces procédés.

Plus particulièrement, l'invention concerne un procédé de sécurisation utilisant un support portatif de données numériques lisible par un appareil électronique utilisateur qui comprend au moins une interface d'entrée et un écran, le support de données comportant un dispositif électronique de sécurisation qui comprend :

- une interface de réception comprenant au moins un capteur optique pour recevoir des informations d'entrée provenant de l'appareil électronique utilisateur,
- une interface d'émission adaptée pour émettre des informations de sortie en fonction des informations d'entrée reçues, ces informations de sortie correspondant (directement ou indirectement) à un code de sécurisation destiné à être communiqué à l'interface d'entrée de l'appareil électronique utilisateur,
- et une unité centrale électronique reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission,

le procédé de sécurisation comprenant les étapes suivantes :

(a) faire transmettre les informations d'entrée par le dispositif électronique utilisateur à l'interface de réception du support de données,

(b) faire déterminer les informations de sortie par l'unité centrale du support de données, en fonction

des informations d'entrée,

(c) faire émettre par l'interface de sortie du support de données, les informations de sortie correspondant au code de sécurisation, et communiquer ce code de sécurisation à l'appareil électronique utilisateur, par l'intermédiaire de l'interface d'entrée dudit appareil électronique utilisateur,

(d) et en fonction du code de sécurisation reçu par l'appareil électronique utilisateur, autoriser ou non certaines opérations réalisées au moyen dudit appareil électronique utilisateur (les opérations en question peuvent être réalisées directement par l'appareil électronique utilisateur, ou le cas échéant par un appareil électronique distant relié audit appareil utilisateur).

Le document US-A-5 652 838 décrit un exemple de procédé utilisant un tel support portatif sécurisé de données numériques, constitué en l'occurrence par un disque optique. L'interface d'entrée est constituée par des capteurs optiques adaptés pour détecter le rayon laser de lecture d'un ordinateur utilisant le disque optique, lequel rayon laser est commandé de façon que sa séquence de passage sur les capteurs optiques corresponde à un certain code d'entrée. L'interface de sortie du disque optique est constituée par un écran qui affiche un code de sortie en fonction du code d'entrée reçu de l'ordinateur. L'utilisateur doit sortir le disque optique de son lecteur pour lire le code de sortie, après quoi ledit utilisateur tape ce code sur le clavier de son ordinateur, ce qui autorise l'utilisation du disque optique par l'ordinateur. On se prémunit ainsi contre les copies illicites du disque optique.

Ces dispositions paraissent très séduisantes, puisqu'elles permettent de transmettre des informations vers le disque optique au moyen du faisceau de lecture déjà prévu pour lire ce disque.

Mais lesdites dispositions présentent l'inconvénient d'obliger à placer les capteurs optiques dans la zone de données du disque pour que ces capteurs puissent recevoir le faisceau de lecture, d'où des contraintes quant à la disposition des données dans ladite zone de stockage de données et des limitations de capacité de ladite zone de données.

De plus, cette solution n'est utilisable en pratique que dans le cas où le support de données est à lecture optique.

La présente invention a notamment pour but de pallier ces inconvénients.

A cet effet, selon l'invention, un procédé de sécurisation du genre en question est caractérisé en ce qu'au cours de l'étape (a), on place le capteur optique du disque face à l'écran de l'appareil électronique utilisateur, et on fait émettre par ledit écran un signal lumineux modulé porteur des informations d'entrée.

On évite ainsi les contraintes susmentionnées relatives à la capacité de la zone de données et à la disposition des données dans ladite zone de données, puisqu'il n'est plus obligatoire de placer le capteur optique dans la zone de données lorsque le support de données est un disque optique.

De plus, cette solution technique est utilisable non seulement pour les supports de données à lecture optique, mais également pour d'autres types de supports de données, notamment à lecture magnétique.

Dans des modes de réalisation préférés de l'invention, on peut éventuellement avoir recours en outre à l'une et/ou à l'autre des dispositions suivantes :

- le support de données utilisé est un disque optique comprenant une zone de données annulaire entourant une partie centrale dépourvue de données numériques, laquelle partie centrale comprend le capteur optique ;

- au cours de l'étape (a), ledit signal lumineux modulé est émis dans une zone prédéterminée appartenant à l'écran, et on place le capteur optique du support de données au voisinage immédiat de ladite zone prédéterminée ;

- au cours de l'étape (a), ladite zone prédéterminée de l'écran est signalée par au moins un repère affiché par l'écran ;

- au cours de l'étape (c), les informations de sortie sont émises par le support de données sous forme d'un signal acoustique ;

- le signal acoustique contenant les informations de sortie est écouté par un opérateur humain, lequel opérateur détermine le code de sécurisation en fonction du signal écouté (ledit code de sécurisation peut le cas échéant être constitué par les informations de sortie elles-mêmes) et communique ce code de sécurisation à l'appareil électronique utilisateur par l'intermédiaire de son interface d'entrée ;

- le signal acoustique contenant les informations de sortie est reçu directement par l'interface d'entrée de l'appareil électronique utilisateur ;

- le signal acoustique contenant les informations de sortie est transmis à un poste de contrôle distant qui détermine le code de sécurisation en fonction dudit signal acoustique et transmet ce code de sécurisation à l'interface d'entrée de l'appareil électronique utilisateur ;

- on fait échanger des données codées entre d'une part, un poste central distant communiquant avec l'appareil électronique utilisateur, et d'autre part, l'unité centrale du support de données, par l'intermédiaire des interfaces d'émission et de réception dudit support de données (on peut ainsi notamment identifier l'utilisateur en fonction des données codées échangées entre le poste central distant et l'unité centrale du support de données, pour sécuriser une opération à dis-

tance, par exemple une opération de paiement à distance ou autre) ;

- le dispositif électronique de sécurisation a en mémoire un compte d'unités de valeur, et l'unité centrale dudit dispositif de sécurisation est adaptée pour faire varier ledit compte d'unités de valeur en fonction de données codées reçues et émises par l'unité centrale par l'intermédiaire des interfaces de réception et d'émission ;

- le dispositif électronique de sécurisation a en mémoire au moins un compteur d'unités d'utilisation, et l'unité centrale dudit dispositif de sécurisation fait varier ledit compteur en fonction des mouvements du support de données détectés par un capteur de mouvement ;

- on fait lire le compteur d'unités d'utilisation par un lecteur externe, au moyen d'une interface de communication appartenant audit dispositif de sécurisation.

Par ailleurs, l'invention a également pour objet un disque optique pour la mise en œuvre d'un procédé tel que défini ci-dessus, ce disque comprenant une zone de données annulaire entourant une partie centrale dépourvue de données numériques, ce disque optique étant lisible par un appareil électronique utilisateur au moyen d'un lecteur à faisceau lumineux, lequel appareil électronique utilisateur comprend en outre au moins une interface d'entrée et un écran lumineux, ledit support de données comportant un dispositif électronique de sécurisation qui comprend :

- une interface de réception comprenant au moins un capteur optique disposé dans la partie centrale du disque optique, pour recevoir des informations d'entrée provenant de l'écran de l'appareil électronique utilisateur,

- une interface d'émission adaptée pour émettre des informations de sortie en fonction des informations d'entrée reçues, ces informations de sortie correspondant (directement ou indirectement) à un code de sécurisation

destiné à être communiqué à l'interface d'entrée de l'appareil électronique utilisateur,

- et une unité centrale électronique reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission ;

- le dispositif de sécurisation comporte en outre un capteur de mouvement.

D'autres caractéristiques et avantages de l'invention apparaîtront au cours de la description suivante de plusieurs de ses formes de réalisation, données à titre d'exemples non limitatifs, en regard des dessins joints.

Sur les dessins :

- la figure 1 est une vue schématique d'un micro-ordinateur pouvant utiliser un disque optique selon l'invention, comprenant un circuit électronique de sécurisation,

- la figure 2 est un schéma bloc du circuit électronique de sécurisation du disque optique de la figure 1, dans une première forme de réalisation de l'invention,

- et la figure 3 est une vue similaire à la figure 2, dans une deuxième forme de réalisation de l'invention.

Sur les différentes figures, les mêmes références désignent des éléments identiques ou similaires.

La figure 1 représente un micro-ordinateur 1 comprenant un écran lumineux 1a (écran cathodique, écran à plasma, écran à cristaux liquides rétro-éclairé, etc.), un clavier 1b et un lecteur 2 de disques optiques numériques (CD-ROM, DVD, etc.) ou autres supports de données numériques.

L'invention a notamment pour but de sécuriser l'utilisation du disque optique 3, notamment afin d'empêcher les copies illicites de ce disque optique.

A cet effet, le disque optique 3 comporte, en dehors de sa zone de stockage de données 4 et avantageusement dans sa partie centrale 5 dépourvue de données, un circuit électronique de sécurisation 6.

Ce circuit électronique de sécurisation, qui est représenté sur la figure 2, est intégré dans la matrice de résine du disque optique et comporte :

- une unité centrale électronique 7 (MP) tel qu'un microcontrôleur ou microprocesseur associé à une mémoire 8 (MEM) pouvant être interne audit microcontrôleur ou microprocesseur (on peut utiliser par exemple le microcontrôleur P8WE5032 commercialisé par PHILIPS SEMICONDUCTORS, une division de la société ROYAL PHILIPS ELECTRONICS, Eindhoven, PAYS-BAS, ou encore le microcontrôleur AT89SC commercialisé par la société ATMEL CORPORATION, 2325 Orchard Parkway, San Jose, CA 95131, USA),

- une source d'énergie électrique 9 (BATT.) telle qu'une pile miniaturisée (par exemple, une pile commercialisée sous la marque TMF® par la société BOLDER TECHNOLOGIES CORPORATION, 4403 Table Mountain Drive, Golden, Colorado (CO) 80403, USA), qui alimente le circuit électronique 6,

- au moins un capteur optique 10 (SENS.) tel qu'un phototransistor, une photodiode ou similaire,

- et un transducteur acoustique, de préférence piézo-électrique, tel qu'un haut-parleur ou une sonnerie électronique 11 ("buzzer") commandée par l'unité centrale 7 et émettant par exemple des signaux sonores ayant un spectre de fréquence constant.

Le dispositif qui vient d'être décrit peut mettre en œuvre un procédé de sécurisation qui permet par exemple de vérifier la présence du disque optique 3 original correspondant à une certaine application (programme, base de données, etc.), notamment lors de l'installation initiale de cette application sur le micro-ordinateur 1.

A cet effet, lors de l'exécution par le micro-ordinateur 1 du programme d'installation de l'application considérée, ce programme génère des informations d'entrée telles qu'un premier code aléatoire, qui est transmis par le micro-ordinateur 1 vers le disque optique 3 par l'intermédiaire de l'écran 1a, sous la forme d'un signal lumineux modulé émis par exemple à partir d'une zone émettrice prédéterminée 17 de l'écran.

A cette occasion, le micro-ordinateur peut :

- commander le lecteur 2 façon à faire sortir le disque optique 3 dudit lecteur,
- et faire afficher sur l'écran un message demandant à l'utilisateur de disposer le disque optique 3 avec son circuit de sécurisation 6 placé face à l'écran et de préférence directement contre ledit écran.

Pour favoriser le bon positionnement du disque optique 3 sur l'écran, le micro-ordinateur 1 peut avantageusement faire afficher sur cet écran un repère 18 qui indique le positionnement du disque optique. Il peut s'agir par exemple d'un cercle lumineux 18 correspondant au diamètre externe du disque optique, d'une ou plusieurs flèches à mettre en correspondance avec des flèches ou similaires apposées sur le disque, ou autre. Le trou central du disque 3 pourrait également être utilisé pour être mis en correspondance avec un repère lumineux affiché à l'écran 1a.

De plus, la face du disque optique 3 qui doit être placée à l'opposé de l'écran 1a, et/ou le cas échéant celle qui doit être placée contre l'écran peuvent avantageusement être repérées par un ou plusieurs marquages prédéterminés apposés sur le disque 3.

Les informations d'entrée peuvent être codées par modulation de l'intensité lumineuse émise par la zone émettrice 17 de l'écran, et/ou par modulation des couleurs émises par cette zone 17.

Avantageusement, on peut moduler en parallèle à l'intensité lumineuse des trois couleurs élémentaires de chaque pixel de l'écran 1a : on multiplie ainsi par trois le débit de données échangé entre l'écran 1a et le disque optique 3. Dans ce cas, le capteur optique 10 comportera plusieurs éléments sensibles respectivement aux différentes couleurs élémentaires des pixels de l'écran 1a.

Le débit de données pourrait encore être augmenté en faisant émettre les données en parallèle par plusieurs zones émettrices de l'écran 1a, auquel cas le circuit 6 comporterait autant de capteurs optiques 10 que l'on placerait en correspondance avec les diverses zones émettrices.

Compte tenu des fréquences de balayage d'écran habituellement rencontrées, le débit brut des données ainsi émis par l'écran 1a sera dans tous les cas supérieur à 25 bits/s et par couleur élémentaire, soit au minimum 75 bits/s en utilisant les trois couleurs élémentaires des pixels.

La démodulation du signal lumineux modulé pourra se faire au niveau de l'unité centrale 7, soit par détection de seuils adaptatifs ou non, soit par détection de fronts, de façon connue en soi.

Grâce à cette démodulation, l'unité centrale reconnaît les informations d'entrée qui lui sont communiquées par le capteur optique 10, et détermine des informations de sortie en fonction de ces informations d'entrée : ces informations de sortie peuvent se présenter par exemple sous la forme d'un deuxième code pseudo-aléatoire généré en fonction d'une clé de codage contenue dans la mémoire 8 de l'unité centrale.

Ensuite, l'unité centrale fait émettre les informations de sortie sous la forme d'un signal acoustique par le transducteur 11.

Ce signal acoustique peut comporter plusieurs

trains de signaux sonores (par exemple 3 à 6 trains de signaux sonores) comprenant chacun plusieurs signaux sonores élémentaires rapprochés (séparés l'un de l'autre par exemple par une durée de 0,2 s) et de durée constante. Le nombre de signaux sonores élémentaires de chaque train de signaux sonores est compris entre 1 et un nombre entier prédéterminé n au moins égal à 2 et par exemple égal à 4. Les trains de signaux sonores peuvent être séparés les uns des autres par des périodes de silence au moins égales à une durée prédéterminée (par exemple, ces périodes de silence peuvent être toutes égales à environ 2 s).

Les informations de sortie sont ainsi codées par le nombre de signaux sonores élémentaires de chaque train de signaux sonores.

Le signal acoustique contenant les informations de sortie est écouté par un opérateur humain, lequel opérateur détermine ainsi le deuxième code susmentionné sous la forme d'une suite de chiffres compris chacun entre 1 et n, correspondant respectivement aux nombres de signaux sonores des différents trains de signaux sonores élémentaires successivement émis par le disque 3.

Puis ledit opérateur communique au micro-ordinateur 1 un code de sécurisation fonction dudit deuxième code (en pratique confondu avec ledit deuxième code), par exemple par l'intermédiaire du clavier 1b. Ces opérations sont de préférence guidées par un ou plusieurs messages affichés sur l'écran 1a du micro-ordinateur.

Si le code de sécurisation reçu est bien relié au premier code susmentionné par une relation prédéterminée, le micro-ordinateur 1 autorise alors le déroulement du programme d'installation ; à défaut, il interdit le déroulement normal de ce programme.

Ce contrôle du bon déroulement du programme d'installation peut également être obtenu notamment :

- par un cryptage des données contenues dans le

disque optique 3, le décryptage de ces données ne pouvant être réalisé par le micro-ordinateur qu'avec une clé de décryptage qui est fonction du code de sécurisation susmentionné et du premier code susmentionné,

- ou en incluant dans le programme d'installation ou dans un programme contenu dans le disque optique 3 et destiné à être copié dans la mémoire du micro-ordinateur, un branchement vers une adresse de programmation qui ne peut être déterminée qu'en fonction du code de sécurisation susmentionné et du premier code susmentionné.

Les mêmes principes peuvent être utilisés pour contrôler non plus la seule installation, mais l'usage de l'application informatique considérée, en obligeant l'utilisateur à utiliser le disque optique 3 au moins lors du lancement de ladite application.

Dans ce cas, on notera qu'il est possible en outre de contrôler les modalités d'utilisation de cette application informatique en fonction de données incluses dans la mémoire 8 de l'unité centrale du disque optique 3, et de prévoir que l'unité centrale 7 ne renvoie le deuxième code susmentionné que si les conditions d'utilisation requises sont réunies.

A titre d'exemple, on peut ainsi prévoir :

- un nombre maximum d'utilisations ou une durée maximum d'utilisation de l'application informatique,
- ou encore une date à partir de laquelle l'application informatique ne fonctionne plus sauf à racheter un disque optique 3,
- ou encore une limitation des modules de programme ou de données accessibles à l'utilisateur (dans ce dernier cas, le processus de sécurisation susmentionné doit être répété à chaque fois que l'utilisateur veut accéder à un nouveau module de programme ou de données).

On notera que le signal acoustique émis par le transducteur 11 pourrait être codé autrement que de la fa-

çon décrite ci-dessus, et notamment :

- en faisant émettre ce signal acoustique sous la forme d'une suite de signaux sonores de durées variables séparés les uns des autres par des périodes de silence de durée prédéterminée, les informations de sortie étant codées par la variation de la durée des différents signaux sonores ;

- ou en modulant la fréquence du signal sonore émis (dans ce cas, le spectre de fréquences du transducteur 11 ne doit pas être constant, ce transducteur pouvant prendre la forme d'un haut-parleur piézo-électrique).

En variante, il serait par ailleurs possible de prévoir que le signal acoustique émis par le transducteur 11 soit reçu directement par le micro-ordinateur 1, notamment par l'intermédiaire d'un microphone 12 externe qui est connecté à une carte son interne du micro-ordinateur et qui est approché du lecteur 2 par l'utilisateur au moment opportun, en fonction des indications données sur l'écran 1a du micro-ordinateur.

En pratique, le poste distant 13 peut être constitué notamment par un site internet.

Selon une autre variante, le signal acoustique émis par le transducteur 11 est transmis à un poste de contrôle distant 13 :

- par l'intermédiaire du microphone 12 susmentionné et d'un modem 14 appartenant au micro-ordinateur 1 et relié au poste de contrôle distant 13 par l'intermédiaire du réseau téléphonique commuté,

- ou par l'intermédiaire de l'utilisateur téléphonant au poste de contrôle 13.

Dans ce dernier cas, le poste de contrôle distant 13 détermine le code de sécurisation en fonction dudit signal acoustique et transmet ce code de sécurisation au micro-ordinateur 1 par l'intermédiaire du modem 14 (ou bien le code de sécurisation est donné par téléphone à

l'utilisateur, qui le tape ensuite sur le clavier 1b du micro-ordinateur). Eventuellement, le poste de contrôle distant 13 peut être amené à ne pas transmettre ce code de sécurisation au micro-ordinateur 1, par exemple si l'utilisation de l'application informatique considérée est soumise à un abonnement qui n'a pas été payé.

Selon une autre variante, représentée sur la figure 3, le transducteur acoustique peut être un haut-parleur 16 associé à un circuit de synthèse vocale 15 lui-même commandé par l'unité centrale 7 : dans ce cas, le haut-parleur 16 émet un message sonore compréhensible par l'utilisateur et contenant les informations de sortie qui correspondent au code de sécurisation. Eventuellement, le circuit de synthèse vocale 15 peut être intégré à l'unité centrale 7, constituée par exemple par un microprocesseur de type TSP50C0x/1x commercialisé par la société TEXAS INSTRUMENTS, Dallas, USA.

On notera par ailleurs que le disque optique 3 pourrait comporter une interface d'émission autre qu'une interface acoustique, par exemple une interface optique.

En particulier, les informations de sortie pourraient également être communiquées à l'utilisateur par l'intermédiaire d'un afficheur 23, en remplacement ou en complément du transducteur 11 ou du haut-parleur 16.

On notera enfin que le processus de sécurisation autorisé par le disque optique 3 ou autre support de données selon l'invention n'est pas limité au contrôle de l'utilisation de programmes ou de données contenus dans le disque optique : au contraire, ce processus de sécurisation peut être utilisé par exemple pour identifier l'utilisateur, notamment pour permettre des opérations de paiement à distance ou pour permettre un accès à distance à des données protégées, et ce sans qu'il soit nécessaire de doter le micro-ordinateur d'un dispositif de sécurisation spécifique tel qu'un lecteur de cartes à mémoire ou simi-

laire.

Dans ce cas, lorsque le micro-ordinateur 1 est doté d'un microphone 12 et d'un modem 14, le processus de sécurisation débute par l'entrée d'un code secret par l'utilisateur sur le clavier 1b, puis le poste central 13 susmentionné (ou similaire) échange des messages codés avec le circuit de sécurisation 7 du disque optique, pour vérifier la cohérence entre le code entré par l'utilisateur et une clé secrète contenue dans la mémoire 8 de l'unité centrale 7, comme cela est déjà connu pour les cartes de paiement à mémoire.

Un tel paiement à distance pourra être utilisé par exemple pour accéder à de nouvelles fonctionnalités d'un logiciel mémorisé sur le disque optique 3, ou payer une location du logiciel porté par le disque 3. Dans ces deux cas, le poste central 13 (en pratique, un site internet) enverra un code d'accès au micro-ordinateur 1, lequel demandera à l'utilisateur de placer le disque 3 face à l'écran 1a pour pouvoir transférer ce code au circuit de sécurisation 6 du disque par le biais du capteur optique 10. Ce code sera ensuite utilisé par le circuit 6 pour élaborer les informations de sortie en réponse aux informations d'entrée, à chaque nouvel accès de l'utilisateur auxdites nouvelles fonctionnalités ou au logiciel dans son ensemble.

On pourrait également utiliser un support de données sécurisé tel que décrit ci dessus comme porte-monnaie électronique ou similaire. Dans ce cas, le dispositif électronique de sécurisation 6 peut avoir en mémoire un compte d'unités de valeur (unités monétaires ou similaires), et l'unité centrale 7 dudit dispositif de sécurisation est alors adaptée pour faire varier ledit compte d'unités de valeur en fonction de données codées reçues et émises par l'unité centrale 7 par l'intermédiaire des interfaces de réception et d'émission, par exemple pour re-

charger le compte lors d'un rachat d'unités de valeurs par l'utilisateur ou au contraire pour débiter le compte en fonction d'achats ou d'autres opérations payantes effectuées par l'utilisateur, par exemple sur le réseau internet.

Lorsqu'on utilise le dispositif de sécurisation 6 pour contrôler ou limiter l'usage du support de données, comme déjà indiqué ci-dessus, ou pour établir un profil d'utilisateur, ce dispositif électronique de sécurisation peut également avoir en mémoire un ou plusieurs compteurs d'unités d'utilisation.

Lorsqu'il s'agit de limiter l'usage du support de données, ce compteur peut être représentatif par exemple d'un nombre d'utilisations, et l'unité centrale 7 dudit dispositif de sécurisation peut être adaptée pour incrémenter ou décrémenter ledit compteur en fonction des mises en fonctionnement du support de données, lesquelles peuvent correspondre à des réceptions de signaux optiques modulés par le capteur 10 ou à des détections de rotation du disque 3 par un capteur de mouvement tel qu'un accéléromètre miniature 19 (ACC.) qui pourrait le cas échéant être intégré au disque 3. Par exemple, l'interface d'émission du dispositif de sécurisation cesse d'émettre les informations codées de sortie qui permettent normalement à l'appareil utilisateur de faire fonctionner le support de données lorsque l'unité centrale 7 a détecté un nombre x prédéterminé de mises en fonctionnement du support de données, c'est-à-dire lorsque le compteur atteint x en partant de 0 ou lorsqu'il atteint 0 en partant de x.

Le capteur 19 pourra par exemple être un microcapteur (pouvant présenter par exemple une surface de 2 mm sur 2 mm) obtenu par micro-usinage sur silicium, tels que les capteurs 2g et 50g réalisés par le Laboratoire d'Electronique, de Technologie et d'Instrumentation (LETI) du CEA (COMMISSARIAT A L'ENERGIE ATOMIQUE), FRANCE.

Lorsqu'il s'agit d'établir un profil d'utilisateur, le ou les compteurs d'utilisation peuvent par exemple être incrémentés à chaque fois que le disque 3 reçoit un signal optique modulé de l'écran 1a pour accéder à certains modules logiciels, ou lorsque le capteur de mouvement 19 détecte certains mouvements ou certaines suites prédéterminées de mouvements, représentatifs de certaines opérations prédéterminées.

Avantageusement, on peut faire lire le compteur d'unités d'utilisation par un lecteur externe 22 (EXT DRV - figure 2), au moyen d'une interface de communication 21 telle qu'une étiquette électronique (TAG) adaptée pour communiquer avec le lecteur 22 par voie hertzienne et appartenant audit dispositif de sécurisation 6. Une telle lecture du compteur d'utilisation pourra avoir lieu par exemple lors du passage de l'utilisateur dans un magasin commercialisant le support de données. Dans ce cas, le support de données pourra avantageusement être miniaturisé, par exemple au format d'une carte de crédit.

Lorsque le circuit de sécurisation 6 comporte un capteur de mouvement 19, l'unité centrale 7 pourrait le cas échéant être conçue pour bloquer le fonctionnement du circuit 6 lorsque le capteur de mouvement 19 a détecté certains mouvements où certaines séquences de mouvements, par exemple un mouvement de rotation continue pendant une durée supérieure à une limite prédéterminée. Dans ce cas, il pourrait alors être possible de débloquer le fonctionnement du circuit de sécurisation 6 en se connectant à un poste centrale distant 13, par exemple un site internet, et en faisant générer à partir de ce poste central distant un signal codé émis par l'écran 1a de l'ordinateur sous forme d'un signal lumineux modulé qui est reçu par le capteur optique 10.

REVENDICATIONS

1. Procédé de sécurisation utilisant un support portatif de données numériques (3) lisible par un appareil électronique utilisateur (1) qui comprend au moins une interface d'entrée (1b, 12) et un écran (1a), le support de données (3) comportant un dispositif électronique de sécurisation (6) qui comprend :

- une interface de réception comprenant au moins un capteur optique (10) pour recevoir des informations d'entrée provenant de l'appareil électronique utilisateur,
- une interface d'émission (11, 16) adaptée pour émettre des informations de sortie en fonction des informations d'entrée reçues, ces informations de sortie correspondant à un code de sécurisation destiné à être communiqué à l'interface d'entrée (1b, 12) de l'appareil électronique utilisateur,
- et une unité centrale électronique (7) reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission,

le procédé de sécurisation comprenant les étapes suivantes :

(a) faire transmettre les informations d'entrée par le dispositif électronique utilisateur (1) à l'interface de réception (10) du support de données,

(b) faire déterminer les informations de sortie par l'unité centrale (7) du support de données, en fonction des informations d'entrée,

(c) faire émettre par l'interface de sortie (11, 16) du support de données, les informations de sortie correspondant audit code de sécurisation, et communiquer ce code de sécurisation à l'appareil électronique utilisateur, par l'intermédiaire de l'interface d'entrée (1b, 12)

dudit appareil électronique utilisateur,

(d) et en fonction du code de sécurisation reçu par l'appareil électronique utilisateur, autoriser ou non certaines opérations réalisées au moyen dudit appareil électronique utilisateur,

caractérisé en ce qu'au cours de l'étape (a), on place le capteur optique (10) du support de données face à l'écran (1a) de l'appareil électronique utilisateur, et on fait émettre par ledit écran un signal lumineux modulé porteur des informations d'entrée.

2. Procédé selon la revendication 1, dans lequel le support de données utilisé est un disque optique (3) comprenant une zone de données annulaire (4) entourant une partie centrale (5) dépourvue de données numériques, laquelle partie centrale comprend le capteur optique (10).

3. Procédé selon la revendication 1 ou la revendication 2, dans lequel, au cours de l'étape (a), ledit signal lumineux modulé est émis dans une zone prédéterminée (17) appartenant à l'écran, et on place le capteur optique (10) du support de données au voisinage immédiat de ladite zone prédéterminée.

4. Procédé selon la revendication 3, dans lequel, au cours de l'étape (a), ladite zone prédéterminée (17) de l'écran est signalée par au moins un repère (18) affiché par l'écran (1a).

5. Procédé selon l'une quelconque des revendications précédentes, dans lequel, au cours de l'étape (c), les informations de sortie sont émises par le support de données (3) sous forme d'un signal acoustique.

6. Procédé selon la revendication 5, dans lequel le signal acoustique contenant les informations de sortie est écouté par un opérateur humain, lequel opérateur détermine le code de sécurisation en fonction du signal écouté et communique ce code de sécurisation à l'appareil électronique utilisateur par l'intermédiaire de son inter-

face d'entrée (1b).

7. Procédé selon la revendication 5, dans lequel le signal acoustique contenant les informations de sortie est reçu directement par l'interface d'entrée (12) de l'appareil électronique utilisateur.

8. Procédé selon l'une quelconque des revendications 5 à 7, dans lequel le signal acoustique contenant les informations de sortie est transmis à un poste de contrôle distant (13) qui détermine le code de sécurisation en fonction dudit signal acoustique et transmet ce code de sécurisation à l'interface d'entrée de l'appareil électronique utilisateur.

9. Procédé selon l'une quelconque des revendications précédentes, dans lequel on fait échanger des données codées entre d'une part, un poste central (13) distant communiquant avec l'appareil électronique utilisateur (1), et d'autre part, l'unité centrale (7) du support de données, par l'intermédiaire des interfaces d'émission et de réception (11, 16 ; 10) dudit support de données.

10. Procédé selon l'une quelconque des revendications précédentes, dans lequel le dispositif électronique de sécurisation (6) a en mémoire un compte d'unités de valeur, et l'unité centrale (7) dudit dispositif de sécurisation est adaptée pour faire varier ledit compte d'unités de valeur en fonction de données codées reçues et émises par l'unité centrale par l'intermédiaire des interfaces de réception et d'émission (11, 16 ; 10).

11. Procédé selon l'une quelconque des revendications précédentes, dans lequel le dispositif électronique de sécurisation (6) a en mémoire au moins un compteur d'unités d'utilisation, et l'unité centrale (7) dudit dispositif de sécurisation fait varier ledit compteur en fonction des mouvements du support de données détectés par un capteur de mouvement (10).

12. Procédé selon la revendication 11, dans lequel

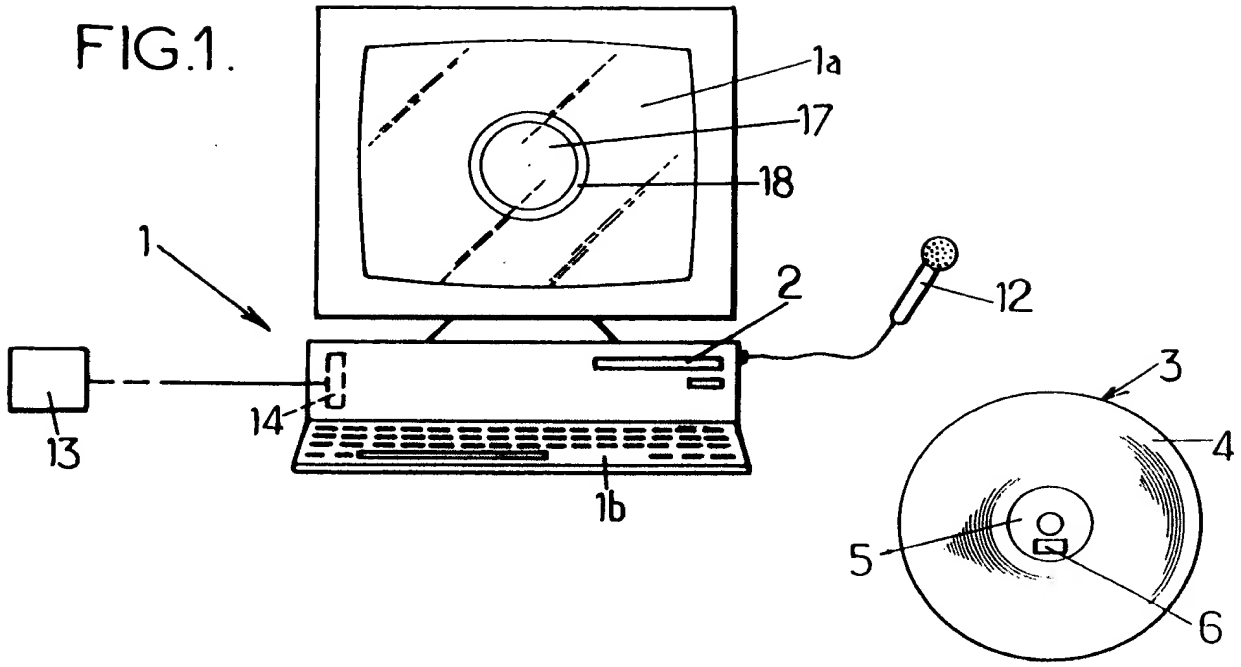
on fait lire le compteur d'unités d'utilisation par un lecteur externe (22), au moyen d'une interface de communication (21) appartenant audit dispositif de sécurisation (6).

13. Disque optique (3) pour la mise en œuvre d'un procédé selon l'une quelconque des revendications précédentes, ce disque comprenant une zone de données annulaire (4) entourant une partie centrale (5) dépourvue de données numériques, ce disque optique étant lisible par un appareil électronique utilisateur (1) au moyen d'un lecteur (2) à faisceau lumineux, lequel appareil électronique utilisateur comprend en outre au moins une interface d'entrée (1b, 12) et un écran lumineux (1a), ledit support de données comportant un dispositif électronique de sécurisation qui comprend :

- une interface de réception comprenant au moins un capteur optique (10) disposé dans la partie centrale (5) du disque optique, pour recevoir des informations d'entrée provenant de l'écran (1a) de l'appareil électronique utilisateur,
- une interface d'émission (11, 16) adaptée pour émettre des informations de sortie en fonction des informations d'entrée reçues, ces informations de sortie correspondant à un code de sécurisation destiné à être communiqué à l'interface d'entrée (1b, 12) de l'appareil électronique utilisateur,
- et une unité centrale électronique (7) reliée aux interfaces de réception et d'émission et adaptée pour déterminer les informations de sortie en fonction des informations d'entrée et pour faire émettre lesdites informations de sortie par l'interface d'émission.

14. Disque optique selon la revendication 13, dans lequel le dispositif de sécurisation (6) comporte en outre un capteur de mouvement (19).

FIG.1.



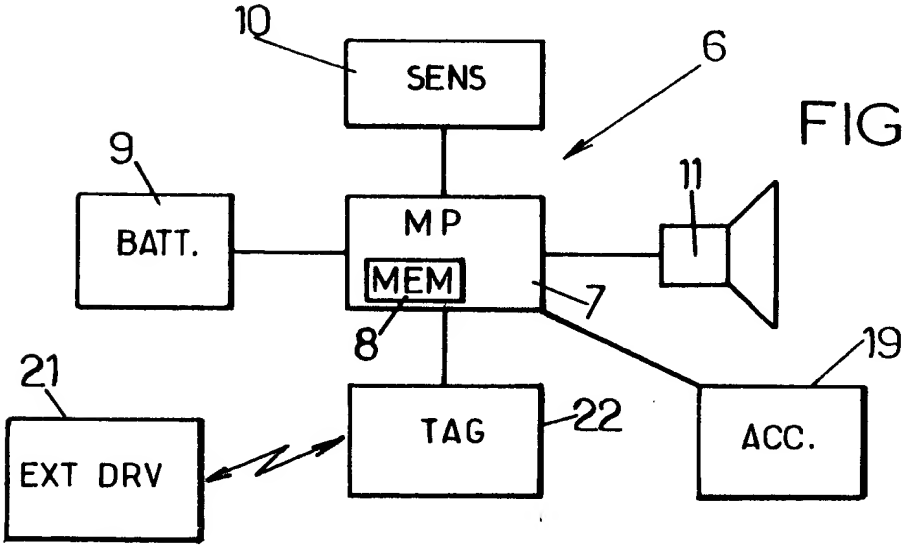


FIG.2.

FIG.3.